Mise en place d'un VPN Client

Introduction

Un réseau privé virtuel (Virtual Private Network en anglais, abrégé en VPN) est une abstraction permettant de considérer plusieurs ordinateurs distants comme étant sur le même réseau local. L'entreprise oXya ce sert de ce système pour pouvoir communiquer avec leurs clients et pouvoir administrer et configurer les équipements des clients à distance.

I Préparation des équipements avant l'installation du VPN

Reset de la configuration des équipements

Pour remettre la configuration des équipements à zéro, nous branchons un câble console à l'équipement et nous nous connectons dessus grâce à un HyperTerminal télécharger au préalable avant. Nous nous mettons en mode privilégié grâce à la commande « enable » pour pouvoir faire les modifications nécessaires. Nous entrons la commande « configuration terminal » et nous tapons la commande « write erase » pour supprimer les anciennes configurations de l'équipement. Nous sauvegardons les modifications grâce à la commande « write memory » et nous redemarrons l'équipement grâce à la commande « reload ».

Reset du mot de passe

Redémarrer le routeur puis appuyer sur la touche « échap ». On rentre en mode « rommon » et on entre la commande « confreg 0x41 ». On rentre ensuite la commande « boot » et on retourne en mode normal. On tape « enable » et « password : xxxx ». On enregistre grâce à la commande « write memory » puis on tape la commande « config-register 0x01 ». On enregistre de nouveau avec la commande « write memory » et on redémarre l'équipement avec la commande « reload »

Mise à jour des équipements

Pour se faire nous installons un serveur TFTP qui nous permettra de télécharger les mises à jour sur les équipements concernés. Nous entrons les commandes ci-dessous et nous renseignons l'adresse ip de notre ordinateur que nous avons configuré avant la manipulation.

```
ciscoasa# copy tftp flash

Address or name of remote host []? 192.168.2.2

Source filename []? asdm-714.bin

Destination filename [asdm-714.bin]? disk0

%Warning:There is a file already existing with this name
Do you want to over write? [confirm]

ciscoasa# copy tftp flash

Address or name of remote host [192.168.2.2]?

Source filename [asdm-714.bin]?

Destination filename [asdm-714.bin]?

Accessing tftp://192.168.2.2/asdm-714.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

L'équipement va donc aller chercher le fichier permettant la mise à jour sur le serveur TFTP et le télécharger. Pour lancer cette nouvelle mise à jour au démarrage de l'équipement, il suffit de taper la commande « boot system disk0:/(nom du fichier) » puis sauvegarder avec la commande « write memory » et redémarrer l'équipement avec la commande « reload ».

Création des VLANs

Pour créer les VLANs nécessaires au bon fonctionnement de la maquette, nous devons configurer les interfaces VLANs et leurs attribuer une adresse IP. Nous rentrons en mode « configuration terminal » et nous créons le VLAN désiré en tapant « interface VLAN10 ». Nous lui attribuons une adresse IP et un masque.

```
Switch(config)#int vlan10
Switch(config-if)#ip address 192.168.1.3 255.255.255.0
Switch(config-if)#no sh
Switch(config-if)#exit
```

Ensuite nous attribuons au port Ethernet du Switch un mode « Access » au VLAN concerné. Nous n'oublions pas de faire un « no shutdown » pour que le port Ethernet ne soit pas éteint.

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface GigabitEthernet0/1
Switch(config-if)#sw
Switch(config-if)#switchport access Vlan 20
Switch(config-if)#description fwa interface 0/0
Switch(config-if)#interface GigabitEthernet0/2
Switch(config-if)#sw
Switch(config-if)#description fwa interface 0/1
Switch(config-if)#
Switch(config-if)#interface GigabitEthernet0/3
Switch(config-if)#sw
Switch(config-if)#switchport access Vlan 20
Switch(config-if)#sw
Switch(config-if)#switchport mode access
Switch(config-if)#description fwb interface 0/0
Switch(config-if)#interface GigabitEthernet0/4
Switch(config-if)#sw
Switch(config-if)#switchport access Vlan 30
Switch(config-if)#switchport mode access
Switch(config-if)#description fwb interface 0/1
Switch(config-if)#
Switch(config-if)#interface GigabitEthernet0/5
Switch(config-if)#sw
Switch(config-if)#switchport access Vlan 20
Switch(config-if)#swi
Switch(config-if)#switchport mode access
Switch(config-if)#description pc
Switch(config-if)#
```

Adressage IP des firewalls

Même manipulation pour les trois firewalls, nous créons les interfaces VLANs, nous leurs attribuons un nameif « inside » ou « outside » et nous leurs attribuons une adresse ip et un masque. Nous configurons par la suite les ports Ethernets qui seront les ports d'entrées et sorties des VLANs créés précédemment.

```
ciscoasa# conf t
ciscoasa(config)# interface Vlan 20
ciscoasa(config-if)# nameif Outside
INFO: Security level for "Outside" set to 0 by default.
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# interface Ethernet0/0
ciscoasa(config-if)# switchport access Vlan 20
ciscoasa(config-if)# int
ciscoasa(config-if)# interface Vlan 10
ciscoasa(config-if)# nameif Inside
INFO: Security level for "Inside" set to 100 by default.
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# INT
ciscoasa(config-if)#
ciscoasa(config-if)# interface Ethernet0/1
ciscoasa(config-if)# switchport access Vlan 10
ciscoasa(config-if)# exit
```

Pour le firewall PIX 501, nous procédons aux mêmes manipulations et nous intégrons une route « Inside » pour qu'il puisse communiquer avec le firewall B.

```
pixfirewall(config)# route ?
Usage:  [no] route <if_name> <foreign_ip> <mask> <gateway> [<metric>]
pixfirewall(config)# route Inside 0.0.0.0 255.255.255.0 192.168.2.1
pixfirewall(config)#
```

Mise en place du SSH

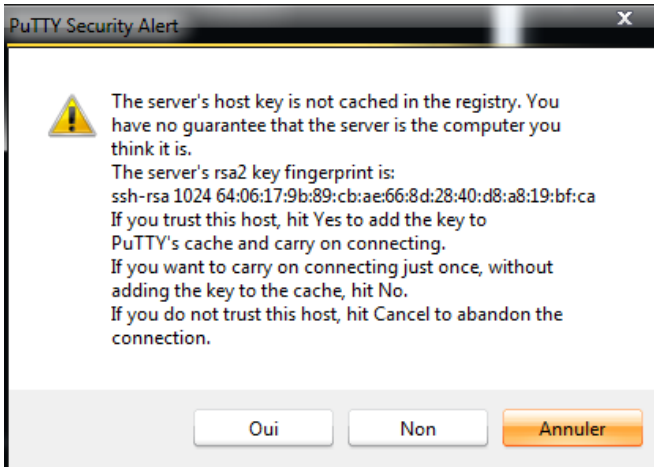
Tout d'abord veuillez vous mettre en mode configuration et veuillez créer le mot de passe d'accès au firewall ainsi que celui du mode « enable » grâce aux commandes « passwd xxx » et « enable secret xxx ». Ensuite nous configurons les noms de domaine de notre firewall avec la commande « ip Domain-name xxxx » Il faut ensuite définir les IP pour qui le matériel réseau sera accessible en ssh. Dans notre exemple nous allons définir la plage IP la plus étendue avec la commande « ssh 0.0.0.0 0.0.0.0 inside ». Pour plus de sécurité nous définissons une durée maximale d'inactivité avant que la connexion ssh au firewall soit interrompue grâce à la commande « ssh timeout 5 ».Le ssh étend basé sur un système de clés, nous générons les clés grâce à la commande « Crypto key generate rsa modulus 1024 ». Nous sauvegardons la manipulation dans la mémoire flash du firewall avec la commande « write memory ».

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#username?
username

Switch(config)#username admin
Switch(config)#line vty 0 15
Switch(config-line)#transport input ssh
Switch(config-line)#login local
Switch(config-line)#crypto key generate rs
Switch(config-line)#crypto key generate rsa
% Please define a domain-name first.
Switch(config)#domain-name oxya.com
                ^
% Invalid input detected at '^' marker.

Switch(config)#ip domain-name oxya.com
Switch(config)#crypto key generate rsa
The name for the keys will be: Switch.oxya.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)
```

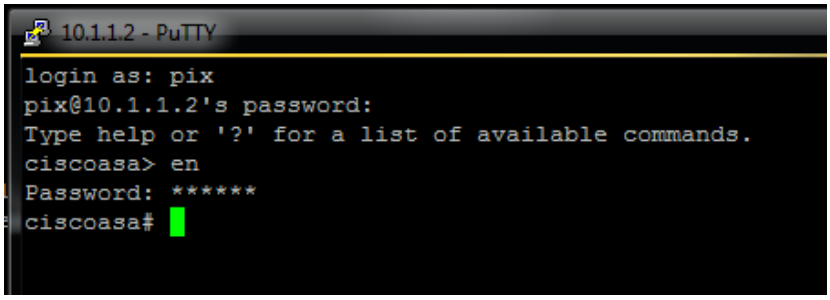
Test de la mise en place du SSH

Avec notre HyperTerminal, nous rentrons l'adresse IP de l'équipement auquel on veut se connecter et nous cochons la case « ssh ». Un message nous informe que l'équipement détient une connexion

ssh et que ce protocole de connexion impose un échange de clés de chiffrement en début de connexion.



Nous arrivons ensuite sur l'interface de l'équipement qui nous demande de renseigner le login, le mot de passe utilisateur et le mot de passe super utilisateur que nous avons configurer un peu plus haut.



II Création d'un VPN client

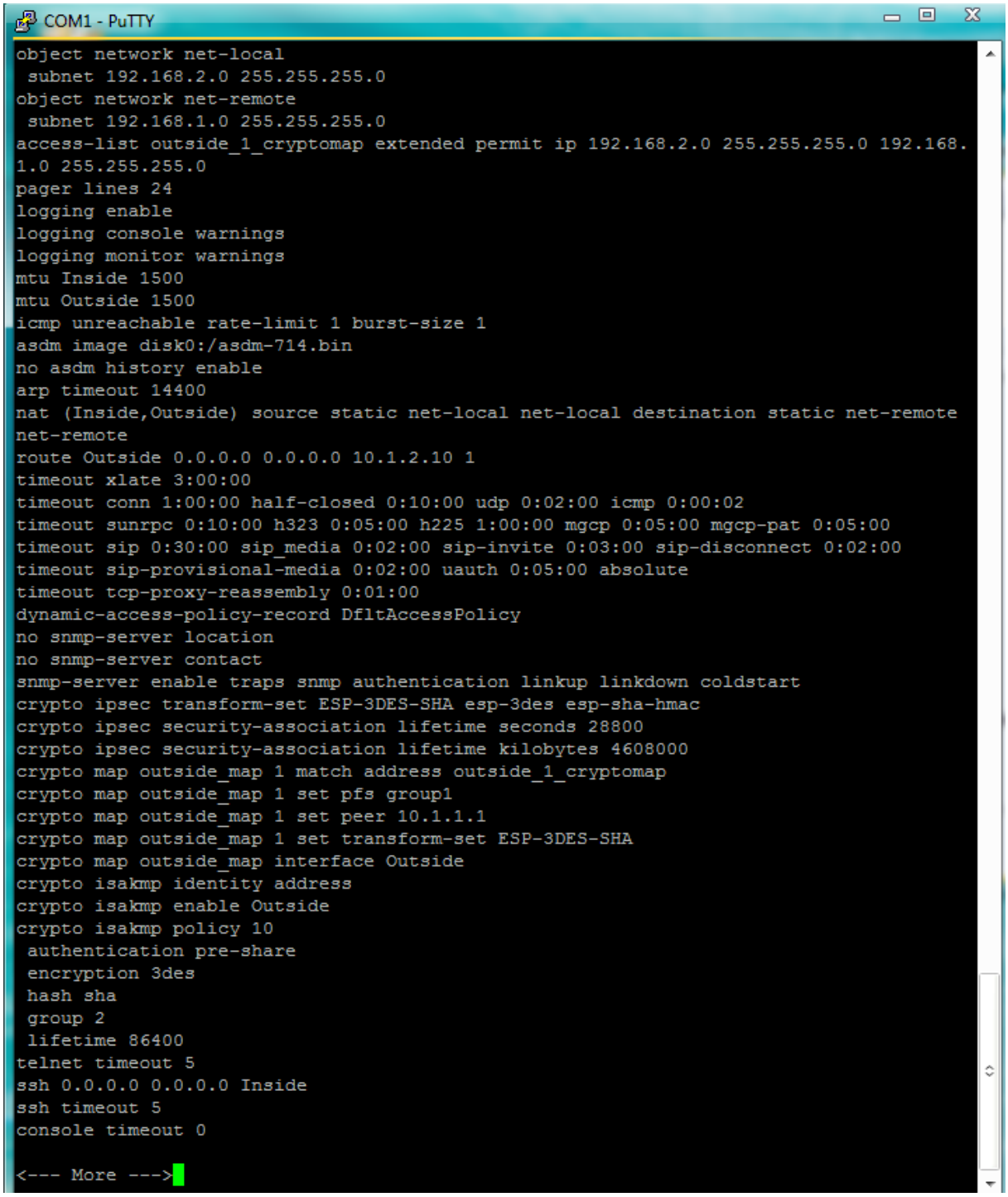
Création d'un VPN sur le firewall A

Nous créons le VPN entre le firewall A et le firewall B pour que la communication entre les deux éléments qui ne sont pas dans le même réseau puissent communiquer. Nous renseignons les deux réseaux qui doivent communiquer, ici il s'agit du réseau « 192.168.1.0/24 » et du réseau « 192.168.2.0/24 » puis nous renseignons les adresses IP par lequel ce VPN doit passer, soit l'adresse IP outside du firewall A et du firewall B. Il faut également attribuer des « access-list » ou entrée de contrôle d'accès donnant ou supprimant des droits d'accès à une personne ou un groupe.

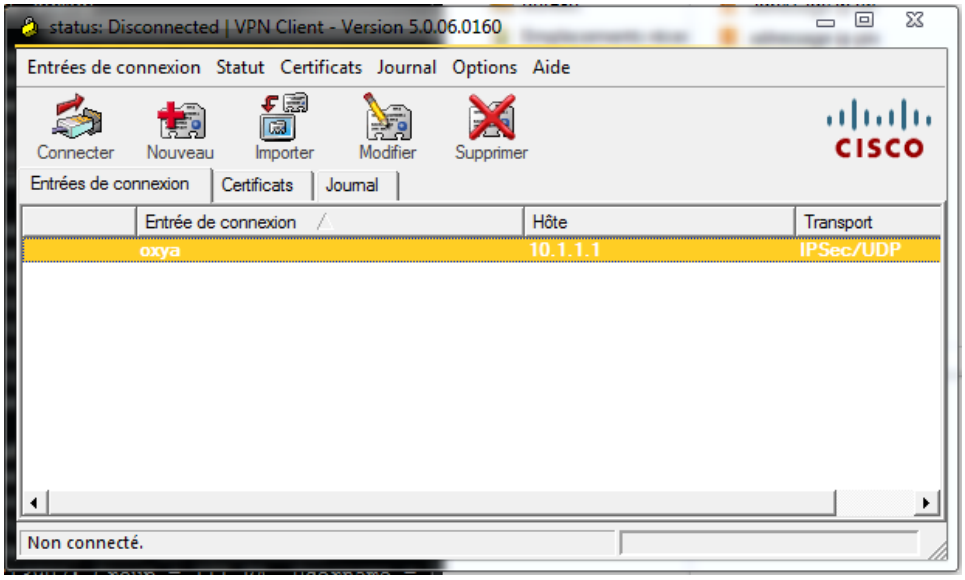
```
ciscoasa# conf t
ciscoasa(config)# object network net-local
ciscoasa(config-network-object)# subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)# object network net-remote
ciscoasa(config-network-object)# subnet 192.168.2.0 255.255.255.0
ciscoasa(config-network-object)# access-list outside_1_cryptomap permit ip 192$
ciscoasa(config)# tunnel-group 10?

configure mode commands/options:
  WORD < 65 char
ciscoasa(config)# tunnel-group 10.1.1.2 type ipsec-l2l
ciscoasa(config)# tunnel-group 10.1.1.2 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# pre-shared-key pass1234
ciscoasa(config-tunnel-ipsec)# isakmp keepalive threshold 10 retry 2
ciscoasa(config-tunnel-ipsec)# crypto isakmp enable outside
ciscoasa(config)# crypto isakmp policy 10 authentication pre-share
ciscoasa(config)# crypto isakmp policy 10 encrypt 3des
ciscoasa(config)# crypto isakmp policy 10 hash sha
ciscoasa(config)# crypto isakmp policy 10 group 2
ciscoasa(config)# crypto isakmp policy 10 lifetime 86400
ciscoasa(config)# crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
ciscoasa(config)# crypto map outside_map 1 match address outside_1_cryptomap
ciscoasa(config)# crypto map outside_map 1 set pfs group1
ciscoasa(config)# crypto map outside_map 1 set peer 10.1.1.2
ciscoasa(config)# crypto map outside_map 1 set transform-set ESP-3DES-SHA
ciscoasa(config)# crypto map outside_map interface outside
ERROR: unable to find interface "outside"
ciscoasa(config)# nat (inside,outside) 1 source static net-local net-local des$
ciscoasa(config)# route outside 0 0 10.1.1.1
ciscoasa(config)# crypto map outside_map interface outside
```

Création d'un VPN client

Ligne de commande pour créer le VPN client sur le firewall A :



Nous installons le logiciel VPN Client Systems Cisco pour permettre au client VPN propriétaire de pouvoir se connecter au VPN.



Test de l'installation

Nous procédons ensuite au câblage entre les différents équipements et nous procédons a la commande « ping » pour voir si les différents équipements communiquent entre eux. Nous faisons une requête ping entre l'ordinateur portable et le firewall pix 501 et nous constatons que la communication se fait.

```
C:\Users\Mélina>ping 192.168.2.2

Envoi d'une requête 'Ping'  192.168.2.2 avec 32 octets de données :
Réponse de 192.168.2.2 : octets=32 temps=1 ms TTL=255
Réponse de 192.168.2.2 : octets=32 temps=1 ms TTL=255
Réponse de 192.168.2.2 : octets=32 temps=1 ms TTL=255
Réponse de 192.168.2.2 : octets=32 temps=1 ms TTL=255

Statistiques Ping pour 192.168.2.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```